CLAIMS

WHAT IS CLAIMED IS:

[c1] 1. A method for secure wireless communication using spread spectrum principles, comprising:

generating at least one pseudorandom number (PN) sequence;
encrypting the PN sequence to render an encrypted PN sequence; and
using the encrypted PN sequence to spread a communication signal.

[c2] 2. The method of Claim 1, wherein the communication signal is received from a data modulation component including a Walsh modulator.

[c3] 3. The method of Claim 1, wherein the PN sequence is encrypted by combining the PN sequence with at least one encryption sequence.

[c4] 4. The method of Claim 1, wherein one or more PN sequences are encrypted by combining the PN sequences with at least one encryption sequence.

[c5] 5. The method of Claim 3, wherein the encryption sequence is generated by a DES or triple-DES encryption.

[c6] 6. The method of Claim 5, wherein the DES or triple-DES encryption receives input including at least one multi-bit key and at least one time varying input.

[c7] 7. The method of Claim 6, wherein the key is periodically refreshed.

[c8] 8. A wireless communication system, comprising:

at least one data modulation component coding a communication signal for error correction to produce a coded signal, interleaving bits in the coded signal to produce an interleaved coded signal to reduce the effect of error bursts, and modulating the interleaved coded signal using a Walsh function to produce a Walsh-modulated interleaved coded signal; and at least one carrier modulator for spreading the Walsh-modulated interleaved coded signal with a pseudorandom number (PN) sequence encrypted with at least one encryption sequence.

[c9] 9. The system of Claim 8, comprising a PN generator generating the PN sequence and receiving the encryption sequence.

[c10] 10. The system of Claim 8, comprising using two encryption sequences.

[c11] 11. The system of Claim 8, comprising an encryption sequence generator generating the encryption sequence.

[c12] 12. The system of Claim 11, wherein the encryption sequence generator includes a DES or triple-DES encryption.

[c13] 13. The system of Claim 11, wherein the encryption sequence generator periodically receives refresh keys useful in generating the encryption sequence.

[c14] 14. A computer program product, comprising:

means for encrypting a PN sequence; and

means for providing the PN sequence to a spread spectrum communication device for use thereof in spreading or despreading a communication signal.

[c15] 15. The product of Claim 14, wherein the communication device uses CDMA principles.

[c16] 16. A chip for use in a communication device, comprising:

at least one data modulation component including:

at least one channel coder receiving a signal for communication, the channel coder coding the signal for error correction to produce a coded signal;

at least one bit interleaver coupled to the channel coder for interleaving bits in the coded signal to produce an interleaved coded signal to reduce the effect of error bursts;

at least one Walsh modulator coupled to the bit interleaver and modulating the interleaved coded signal using a Walsh function to produce a Walsh-modulated interleaved coded signal; and at least one carrier modulator for spreading the Walsh-modulated interleaved coded signal with a pseudorandom number (PN) sequence encrypted with at least one encryption sequence.

[c17] 17. The chip of Claim 16, comprising a PN generator generating the PN sequence and receiving the encryption sequence.

[c18] 18. The chip of Claim 17, wherein the encryption sequence is a first sequence and the PN generator receives the first sequence and a second encryption sequence, the PN sequence being encrypted with both encryption sequences.

[c19] 19. The chip of Claim 16, comprising an encryption sequence generator generating the encryption sequence.

[c20] 20. The chip of Claim 19, wherein the encryption sequence generator includes a DES or triple-DES encryption.

[c21] 21. The chip of Claim 19, wherein the encryption sequence generator periodically receives refresh keys useful in generating the encryption sequence.

[c22] 22. A chip for use in a communication device, comprising:

at least one PN sequence generator receiving at least one encryption sequence and combining the encryption sequence with a PN sequence to establish a combined sequence;

at least one carrier demodulator despreading a received spread spectrum communication signal using the combined sequence to render a despread signal; and

at least one data demodulation component coupled to the carrier demodulator to Walsh-process the despread signal, the demodulation component also deinterleaving the signal to render a deinterleaved signal and channel-demodulating the deinterleaved signal.

[c23] 23. The chip of Claim 22, wherein the encryption sequence is a first sequence and the PN sequence generator receives the first sequence and a second encryption sequence.

[c24] 24. The chip of Claim 23, comprising an encryption sequence generator generating the encryption sequence.

[c25] 25. The chip of Claim 24, wherein the encryption sequence generator includes a DES or triple-DES encryption.

[c26] 26. The chip of Claim 24, wherein the encryption sequence generator periodically receives refresh keys useful in generating the encryption sequence.

[c27] 27. A method for secure wireless communication using spread spectrum principles, comprising:

receiving at least one encryption sequence;

using the encryption sequence to render an encrypted PN sequence; and

using the encrypted PN sequence to despread a received spread spectrum signal to render a despread signal.

[c28] 28. The method of Claim 27, wherein the despread signal is sent to a Walsh modulator.

[c29] 29. The method of Claim 27, wherein the PN sequence is encrypted by combining the PN sequence with at least one encryption sequence.

[c30] 30. The method of Claim 27, wherein one or more PN sequences are encrypted by combining the PN sequences with at least two encryption sequences.

[c31] 31. The method of Claim 29, wherein the encryption sequence is generated by a DES or triple-DES encryption.

[c32] 32. The method of Claim 31, wherein the DES or triple-DES encryption receives input including at least one multi-bit key and at least one varying input.

[c33] 33. The method of Claim 32, wherein the key is periodically refreshed.

[c34] 34. The method of Claim 32, wherein the varying input is at least one long code state.